Department of Homeland Security Daily Open Source Infrastructure Report for 02 February 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Boston Globe and the Worcester Telegram & Gazette said slips containing the names and credit card numbers of thousands of customers of both newspapers were accidentally delivered with bundles of papers last weekend in Worcester, Massachusetts. (See item 9)
- The U.S. Northern Command recently hosted representatives from more than 40 international, federal, and state agencies for an exercise designed to provoke discussion and determine what governmental actions, including military support, would be necessary in the event of an influenza pandemic in the U.S. (See item 30)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *February 02, Utility Automation & Engineering* — **Florida Power & Light plans to strengthen electric grid against future hurricanes.** Florida Power & Light (FPL) presented to the Florida Public Service Commission its Storm Secure Plan, a five−point program to strengthen the company's electric grid against future hurricanes. Since the end of last year's hurricane season, FPL has been working on initiatives to bolster its electric network, especially in light of forecasts for continued heightened hurricane activity. The highlights of FPL's five−point Storm Secure Plan include hardening the electric network by adopting extreme wind

velocity zone criteria as its new standard for all new distribution construction and system upgrades; converting overhead lines to underground for local government−sponsored conversions; modifying its pole inspection, record−keeping, and reporting so that its more than one million wood poles are inspected on a 10−year cycle; increasing its line−clearing activities by 27 percent in 2006; and continuing its post−hurricane follow−up work to repair or replace distribution, transmission, and substation facilities that were damaged. Additionally, certain near−term work is being performed to strengthen targeted facilities prior to the onset of the 2006 hurricane season.
Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICL E_ID=246971&p=22

2. *February 01, North American Electric Reliability Council* — **Pandemic response guide released.** The North American Electric Reliability Council (NERC) has released the Influenza Pandemic Planning, Preparation, and Response Reference Guide for the Electricity sector. The guide assists electricity sector owners and operators enhance their business continuity plans to meet the threat of an influenza pandemic, and it helps them integrate these plans with other existing plans for effective enterprise−wide recovery. NERC's guide includes an overview of key actions, assigned responsibilities, and expected completion dates to prepare for a public health pandemic. The guide will be revised as a threat evolves.
Guide: http://www.nerc.com/~filez/cipfiles.html
Source: http://www.nerc.com

3. *January 31, Agence France−Presse* — **French nuclear watchdog approves deep waste burial.** A French nuclear safety watchdog has given its cautious approval to a technique that would allow the storage of long−term radioactive waste deep underground, according to a statement. The Institute for Radioprotection and Nuclear Safety (IRSN) gave backing in principle to a method for stocking the waste in underground clay sediments that has been developed in a government laboratory in Bure, eastern France. Commenting on a report submitted by the National Agency for the Management of Nuclear Waste laboratory in December, the IRSN experts found that the scientists' underground storage technique "appears technically feasible." Based on its observations so far, the watchdog said, there would be no reason to refuse safety approval for the plans, were they to be implemented. However, the IRSN said a number of points still needed further clarification, notably the exact methods to be used to prevent any soil contamination from the waste. A 1991 law gave the French authorities 15 years to study ways of storing the most dangerous forms of nuclear waste.
Source: http://news.yahoo.com/s/afp/20060131/sc_afp/franceenergynucl ear_060131192151

4. *January 31, Associated Press* — **American Electric Power files plans to build long power line.** American Electric Power Co. (AEP) filed plans Tuesday, January 31 to build a 550−mile power line stretching from West Virginia to New Jersey intended to increase the availability of electricity at lower costs in the eastern U.S. The company expects to spend about $3 billion to build the line and anticipates it will be in service by 2014 if approved. The plans for the AEP Interstate Project have been filed with the Federal Energy Regulatory Commission and the regional grid operators, PJM Interconnection. "We must move forward and address the current inadequacies of our nation's existing transmission infrastructure," Michael Morris, AEP's chairman, president and chief executive, said in a statement. He continued, "This line will reduce congestion costs, cut line losses, enhance reliability and provide the transmission capacity and flexibility that is critical for construction of new fuel−diverse generation,

including renewables." The power line would allow the transmission of an additional 5,000 megawatts of electricity to the east during times of high demand, spokesperson Melissa McHenry said. Although the main purpose of the new power line is to reduce congestion, McHenry said it also will improve reliability because it will be able to better handle fluctuations.
Source: http://news.yahoo.com/s/ap/20060131/ap_on_bi_ge/aep_power_li ne_2

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *February 01, Defense News* — **Report: U.S. military transformation falls short of broader goals.** The Pentagon has embraced the need for military transformation in combat areas but needs to do much more to meet the goals laid down in the U.S. National Security Strategy, says a new report by the Defense Science Board. The National Security Strategy is “much more than combat objectives or even stability and reconstruction operations,” says the first volume of the report, “Transformation: A Progress Assessment,” dated December 2005. “The set of broader goals are far more demanding, complex, costly, and wide reaching in scope than achieving victory on the battlefield. Meeting the National Security Strategy objectives requires a robust and integrated civilian−DoD, multi−agency capacity as part of a broader strategic focus to enable the full array of available U.S. capabilities to achieve strategic objectives.” The study was commissioned in January 2005 by Michael Wynne, then U.S. undersecretary of defense for acquisitions, to assess the Pentagon’s transformation efforts against the 2003 Transformation Planning Guidance, which included “how we fight, how we do business and how we work with others.” The findings and recommendations of the board are not binding.
Defense Science Board: http://www.acq.osd.mil/dsb/reports.htm
Source: http://www.defensenews.com/story.php?F=1503900&C=america

6. *January 31, Government Accountability Office* — **GAO−06−232: Defense Management: Fully Developed Management Framework Needed to Guide Air Force Future Total Force Efforts (Report).** The Air Force is in the process of transforming its force to meet today’s new and emerging threats. Its “Future Total Force” concept is intended to maximize future capabilities by integrating its active, National Guard, and reserve components to a greater degree. While the Air Force was making force structure decisions and developing its 20−year plan, the Air National Guard embarked on its own “Vanguard” transformation initiative to ensure its role and relevance in the new Air Force. This report discusses (1) the processes and events that surrounded the Air Force’s development of its 20−year force structure plan, including the involvement of key stakeholders and the development of the Guard’s Vanguard initiative, and (2) the extent to which the Air Force is utilizing key results−oriented management tools to guide its effort to identify new missions for the Air National Guard and integrate active and Guard forces as part of its Future Total Force effort. The Government

Accountability Office (GAO) recommends the Secretary of the Air Force take steps to fully develop a management framework, accelerate its approval, and establish an evaluation plan to assess its test initiatives. DoD agreed with the recommendations in this report and has begun implementing them.
Highlights: http://www.gao.gov/highlights/d06232high.pdf
Source: http://www.gao.gov/new.items/d06232.pdf

7. *January 31, InfoBase Publishers, Inc.* — **Defense mergers & acquisitions tallies $38 billion in 2005 deals.** Worldwide defense and aerospace companies announced or completed merger & acquisition (M&A) deals worth more than $38 billion in 2005, reports "Defense Mergers & Acquisitions" (DM&A) in its just−published year−end review. The year saw a total of 377 transactions announced or completed. Stuart McCutchan, editor of the DM&A newsletter, commented: "Deal activity reached a level not seen since 1999's all−time high. 2005 was a year in which a lot of factors came together. First, defense spending is scaling historic highs. Second, the commercial aerospace marketplace is hitting its stride. Third, the rush into the government technology services market sector has reached unprecedented proportions." While industry watchers have noted the increased popularity of stock buybacks and dividend payments, M&A activity continued to be the strategic weapon of choice for companies wanting to move decisively into desirable market niches. Top acquirers like France's SAFRAN, L−3 Communications, and DRS Technologies used M&A activity to drive their top lines far past the levels achievable through organic growth alone. McCutchan concluded: "With deals worth more than $9 billion in the works, 2006 is off to a quick start. We look for another strong year for the industry."
DM&A year−end review is available via subscription:
http://companies.infobasepub.com/about/dmna.lasso?−session=IBP_MainSite:42F941EE13c0930F4AgqMhAF2A68
Source: http://www.defense−aerospace.com/cgi−bin/client/modele.pl?session=dae.17213019.1138807193.Q@DRmcOa9dUAAHiHP1M&modele=jdc_34

8. *January 30, Government Accountability Office* — **GAO−06−211: Defense Acquisitions: DoD Management Approach and Processes Not Well−Suited to Support Development of Global Information Grid (Report).** Department of Defense (DoD) officials currently estimate that the department will spend approximately $34 billion through 2011 to develop the core network of the Global Information Grid (GIG), a large and complex undertaking intended to provide on−demand and real−time data and information to the warfighter. DoD views the GIG as the cornerstone of information superiority, a key enabler of network−centric warfare, and a pillar of defense transformation. A high degree of coordination and cooperation is needed to make the GIG a reality. In prior work the Government Accountability Office (GAO) found that enforcing investment decisions across the military services and assuring management attention and oversight of the GIG effort were key management challenges facing DoD. This report assesses (1) the management approach that DoD is using to develop the GIG and (2) whether DoD's three major decision−making processes support the development of a crosscutting, department−wide investment, such as the GIG. GAO is recommending DoD adopt a management approach with more clearly defined leadership, authority to enforce investment decisions across organizational lines, and accountability for ensuring the objectives of the GIG are achieved. DoD concurred with GAO's recommendation.
Highlights: http://www.gao.gov/highlights/d06211high.pdf

Source: http://www.gao.gov/new.items/d06211.pdf

[Return to top]

Banking and Finance Sector

9. *February 01, Associated Press* — **Newspapers report financial data breach.** The Boston Globe and the Worcester Telegram & Gazette said slips containing the names and credit card numbers of thousands of customers of both newspapers were accidentally delivered with bundles of papers last weekend in Worcester, MA. Officials of the newspapers said 240,000 subscribers may be affected. Richard H. Gilman, publisher of The Boston Globe, said "Immediate steps have been taken internally at the Globe and Telegram & Gazette to increase security around credit card reporting." The Telegram & Gazette said the slips also contained routing information for 1,100 of its customers who pay by check. The financial data was on the backside of paper that had inadvertently been recycled and used for routing slips in 9,000 bundles of the Sunday Telegram & Gazette distributed to retailers and newspaper carriers. On Monday, January 30, a merchant noticed the names and credit card numbers on a routing slip and called the newspapers. "There have been no reports of any unauthorized uses of credit card information," Globe vice president Al Larkin said. The company has notified American Express, Discover, MasterCard, Visa, and any banks whose customers may be effected.
Source: http://www.nytimes.com/aponline/business/AP−Newspapers−Credit−Cards.html?_r=1&oref=slogin

10. *February 01, Gazette (CO)* — **University hit by ID security breach.** Personal information on about 2,500 current and former employees at the University of Colorado at Colorado Springs (UCCS) has been compromised by someone who hacked into a computer and infected it with a virus. Names, Social Security numbers, birth dates, and addresses for employees dating back to 2004 were accessed without authorization Friday, January 27, the university said. Obtaining that information did not appear to be the reason for the attack on the computer in the Personnel Department, officials said. They still urged faculty and staff members to notify credit reporting bureaus of the breach and take other precautions against ID theft. UCCS employees were notified of the breach by e−mail. No one has reported that information was used or stolen. Jerry Wilson, information technology director at UCCS, believes the computer containing the personal data was attacked at random. It was one of seven at UCCS infected by a virus that spread rapidly worldwide Friday, mostly at colleges and universities. The virus caused computers to send messages back and forth, clogging communication lines. Wilson said someone loaded the program onto the Personnel Department’s computer remotely, and the virus would have given them access to the computer’s information.
Source: http://www.gazette.com/display.php?id=1314249&secid=1

11. *January 31, Sacramento Bee (CA)* — **ID thefts target Arco stations.** Credit card information linked to more than 1,000 debit cards swiped at Arco gas stations from Sacramento to Redding, CA, was captured by a "skimming" operation used to withdraw at least $110,000 in cash from ATMs in Northern California casinos. Alleged ring leader Claudiu Hotea, 32, was arrested Tuesday, January 24. Placer County Sheriff's Detective Jim Hudson said, "This is the most sophisticated case I've done...These guys invested money in the equipment to make them the most effective and give them the least exposure." Placer County Sheriff's Lt. George Malim

said the thieves used a skimming device by attaching a discreet, black plastic faceplate to the debit card readers at the gas stations. The device records the debit card number. The facade also has a one−way mirror that hides a camera trained to capture fingers punching in PINs. "They leave it there a few hours, come back, take the devices and upload the information into the computer," Malim said. With the debit card and PINs, suspects then coded magnetic strips of other plastic cards and used them to withdraw cash. An affidavit for Hotea's arrest filed by the Secret Service details how investigators unraveled the scheme.
Source: http://www.sacbee.com/content/news/story/14135897p−14964737c .html

12. *January 31, Reuters* — **China bank officials charged with stealing more than $485 million.** A U.S. grand jury indicted two former Bank of China managers and their wives on Tuesday, January 31 over a complex scheme to defraud the state−owned Chinese bank of $485 million, the Justice Department said. The two couples and the fugitive brother of one of the wives were charged with 15 counts of racketeering, money laundering and fraud, the department said in a statement on the indictment by a federal grand jury in Las Vegas, NV. Bank managers Xu Chaofan and Xu Guojun tried to launder the stolen money through Hong Kong, Canada, the United States, and other countries in a scheme that began in 1991 and ran until 2004, when the couples were arrested, the statement said. The two men created shell corporations in Hong Kong and funneled the Bank of China's money into the fake firms and into numerous personal bank and investment accounts, it said. The two bankers then tried to emigrate to the United States from China with their wives, Kuang Wanfang and Yu Yingyi, by obtaining false identities and entering into sham marriages with naturalized U.S. citizens. The indictment alleges that Kuang's brother, who remains a fugitive, helped the couples launder the money.
Source: http://asia.news.yahoo.com/060131/3/2f1sv.html

13. *January 31, Associated Press* — **Honeywell probes posting of employee information on Internet.** Honeywell International is offering credit monitoring and identity theft insurance to approximately 19,000 current and former employees whose personal information −− including Social Security numbers and bank account information −− was posted on an Internet Website. The company notified employees about the breach within a day of learning of it Friday, January 20, according to spokesperson Robert C. Ferris. He said the company was working with federal and state investigators to determine who posted the data. Ferris said he didn't know whether the posting was the work of a disgruntled employee or resulted from an administrative error or other cause. Incidents like the Honeywell security breach are on the rise as thieves and pranksters take aim on corporate America, according to Ron Teixeira, executive director of the National Cyber Security Alliance. "There are a number of reasons why this could have happened. When it's put out on the Web, hackers do that to show they could get access to the information and show the company their security was lacking. Other times, hackers are actually thieves or try to sell the information to thieves to commit ID theft," he said.
Source: http://www.newsday.com/news/local/wire/newjersey/ny−bc−nj−−honeywell−interne0131jan31,0,3889755.story

[Return to top]

Transportation and Border Security Sector

14.

February 01, Reuters — **United Airlines parent emerges from bankruptcy.** UAL Corp, parent of United Airlines, ended three years in Chapter 11 protection on Wednesday, February 1, wrapping up the most expensive airline bankruptcy in history. The No. 2 U.S. airline, which used its time in protection from creditors to slash costs by $7 billion a year, must now sink or swim in a fiercely competitive industry that is plagued by soaring fuel costs and overcapacity. Experts are divided over UAL's prospects for profitability, and even for survival. If UAL succeeds, its story would resemble that of Continental Airlines, which went bankrupt twice before regaining traction. If it fails, UAL would join a long list of U.S. airlines that died in or after bankruptcy −− including TWA and Pan American. UAL filed for bankruptcy in December 2002, weakened by low−fare competition and a drop−off in air travel following the September 11 terror attacks on the United States. Morningstar analyst Chris Lozier said that for UAL to survive and to be a worthwhile equity investment, it needs the most competitive cost structure in the industry.
Source: http://biz.yahoo.com/rb/060201/airlines_ual.html?.v=1

15. *February 01, Mobile Register (AL)* — **Alabama Port Authority plan addresses demand.** The Alabama State Port Authority board approved a strategic plan Tuesday, January 31, in part to address what a docks officials called an unprecedented increase in potential business. Demand for the port jumped beyond expectations after the November announcement of a partnership among the docks, APM Terminals North America Inc., a subsidiary of the A.P. Moller−Maersk Group, and Terminal Link S.A., a division of CMA CGM S.A., according to state docks spokesperson Judy Adams. The three are partnering to build and operate the Choctaw Point container terminal, a $300 million project under construction just south of downtown Mobile. Higher volumes will affect every aspect of the docks' operation, including its computer systems, finances and personnel, Adams said. Last year the port handled 25,000 containers and is expected to handle up to 50,000 this year, docks director Jimmy Lyons said.
Source: http://www.al.com/business/mobileregister/index.ssf?/base/business/1138789317220460.xml&coll=3

16. *February 01, Thunder Bay* — **Restrictions for Cessna planes.** The Transportation Safety Board of Canada is recommending the model of Cessna cargo plane that crashed while enroute to Thunder Bay last fall, be allowed to fly in nothing more than light icing conditions. The board's report follows an investigation into the October 6 crash of a Cessna 208. The plane had just taken off from Winnipeg when the pilot requested an immediate return due to icing. She was killed minutes later when her plane crashed. Board spokesperson John Cottreau says the Cessna 208 should not be allowed to take off if the flight will take it through areas where anything more than light icing is forecast. Earlier this month, the U.S. National Transportation Safety Board said the aircraft should be grounded in most icing conditions.
Source: http://www.tbsource.com/localnews/index.asp?cid=80101

17. *January 31, Associated Press* — **Frontier plans to form holding company.** Frontier Airlines Inc. on Tuesday, January 31, said it plans to reorganize to form a Delaware holding company, subject to shareholder approval. Under the new structure, Frontier Airlines Inc., a Colorado corporation, will become a wholly owned subsidiary of Frontier Airlines Holdings Inc. Frontier said it has tentatively scheduled a special meeting for March 27 to allow shareholders to vote on the proposed reorganization, which is expected to be tax−free to current stockholders.
Source: http://biz.yahoo.com/ap/060131/frontier_airlines_holding_com pany.html?.v=1

18. *January 31, St. Louis Post Dispatch (MO)* — **Midcoast Aviation sold to Swiss company.** A Swiss company on Tuesday, January 31, said it has agreed to buy Midcoast Aviation, most of whose 850 employees work at St Louis' Lambert Field and at St. Louis Downtown Airport repairing and remodeling business jets. Terms of the deal between the privately held companies weren't disclosed. Executives at Jet Aviation Group of Zurich, Switzerland, said they expect the acquisition of Midcoast to be made final by spring. Midcoast will keep its name and Kurt F. Sutterer will remain as president. The deal nearly doubles Jet Aviation's presence in the United States in terms of employees. Midcoast will remain intact and continue to carry out its previously planned expansion, executives said on a conference call. In recent years, Midcoast's revenue growth has been robust on strong demand for business jets. Midcoast specializes in servicing Gulfstream jets and is the only facility in the United States that is authorized to service Bombardier's Global Express jet.
Source: http://www.stltoday.com/stltoday/business/stories.nsf/0/162AC26A0ADC82D88625710800239AF9?OpenDocument

19. *January 30, Pacific Business News* — **ATA ready to emerge from Chapter 11.** ATA Airlines Inc., which serves Hawaii from Arizona and California, says its bankruptcy judge is ready to allow it to leave bankruptcy. Creditors have approved the reorganization plan and Judge Basil Lorch told ATA executives Monday, January 30, in Indianapolis that he was ready to issue a formal order Tuesday permitting reorganization before the end of February. The plan includes settlement on loans from the federal Air Transportation Stabilization Board. One week ago ATA announced an expansion of its code share alliance with Southwest Airlines, in which it essentially acts as Southwest's extension to Hawaii. ATA said it would move its San Francisco base to Oakland and increase service to Hawaii from Oakland, Los Angeles, and Phoenix.
Source: http://biz.yahoo.com/bizj/060131/1222235.html?.v=2

20. *January 30, St. Louis Post Dispatch (MO)* — **The jet of the future.** A new breed of relatively inexpensive aircraft −− "very light jets," or VLJs for short −− is expected to go into production this year. They weigh as much as a minivan and can fly at jet speed using suburban airstrips. They will open up 5,400 suburban and rural airports around the country to jet travel. The VLJs can land on 3,000−foot runways that now accommodate only propeller aircraft. That will enable flying non−stop to rural outposts where there's no commercial service. The small jets start at about $1 million, less than half the price of the most inexpensive ones in production today. Operating costs range from roughly $250 to $730 an hour, depending on the model. This opens up jet ownership to a class of people who historically could afford first−class airfare but not own their own jets. The jets still need certification from the Federal Aviation Administration. And before flying one, a pilot must have special training. Some air−charter companies are ordering VLJs to begin on−demand air−taxi service, or add to existing charter fleets, in states including Florida and North Dakota.
Source: http://www.stltoday.com/stltoday/business/stories.nsf/0/19A396AA23F773E1862571070019F2CA?OpenDocument

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

21. *January 31, United Press International* — **Virginia to eradicate zebra mussels.** Virginia officials say they will attempt a first: killing all zebra mussels from a large, open body of water. A contractor hired by the state was to begin pumping chemicals into a quarry Tuesday, January 31, to kill the mussels. The zebra mussel, a native of Eastern Europe, can clog industrial water−intake pipes, soil beaches, and drive out native shellfish, the Richmond Times−Dispatch reported. The quarry covers 12 acres and its lake is 93 feet deep. The contractor will pump nearly 300,000 pounds of potassium chloride into the lake. Officials said no one has ever eradicated the mussels from a large body of water. Zebra mussels were discovered in the Great Lakes area in 1988, since spreading rapidly in that region and in the Mississippi River basin. Scientists believe the mussels got into the Great Lakes from ballast water dumped by ships from Europe. It has not been determined how the mussels got into the Virginia quarry.
Source: http://www.upi.com/NewsTrack/view.php?StoryID=20060131−12592 0−6104r

22. *January 31, Corvallis Gazette−Times (OR)* — **Agriculture supply business hit with pesticide violation.** A Tangent, OR, based agricultural supply business has been hit with an Oregon−record fine for violations of state pesticide regulations. The Oregon Department of Agriculture levied a civil penalty of $151,626 against the Cacade division of Western Farm Service for 191 violations that occurred between 2002 and early 2005. According to the department, the violations primarily involved selling restricted−use pesticides to unlicensed applicators at Western Farm Service's Willamette Valley locations and selling restricted−use pesticides without a license. The violations occurred at Western Farm Service stores in Ballston, Carlton, Hopmere, Hubbard, and Rickreall. Restricted−use pesticides are among the more toxic or potentially harmful chemicals used by farmers. Both dealers and applicators must be licensed to ensure the substances are used properly.
Source: http://www.gazettetimes.com/articles/2006/02/01/news/communi ty/wedloc01.txt

[Return to top]

Food Sector

23. *February 01, El Universal (Mexico)* — **Ban relaxed on U.S., Canada beef imports.** Mexico reopened its borders on Tuesday, January 31, to imports of U.S. and Canadian beef containing bone material from cows under the age of 30 months. Mexico banned many cuts of U.S. beef in December 2003 after the discovery of a Washington State animal with mad cow disease. In March 2004, the measure was eased to allow cuts of meat without bone or nerve material. Tuesday´s move removes that ban, on the condition that the meat was processed with methods aimed at reducing the risk of mad cow disease. The ban on meat containing bone will continue in the case of animals older than 30 months.
Source: http://www.eluniversal.com.mx/miami/16824.html

[Return to top]

Water Sector

24. *January 30, Associated Press* — **Prescription drug traces found in recycled Los Angeles−area water.** Water quality officials have found traces of resilient prescription drugs in wastewater that has been filtered and recycled into a Southern California aquifer for eventual use as drinking water, but the amounts are so small that the health effects are unclear. Drugs including antibiotics, antipsychotics, birth−control hormones, Viagra, and Valium routinely turn up in wastewater all over the world because people flush them down their toilets. But medications have also ended up in Los Angeles County's water supplies because of the region's aggressive efforts to turn treated sewage into drinking water. Nearly half a trillion gallons of sewage from three treatment plants have replenished the Central Basin aquifer beneath the San Gabriel Valley east of Los Angeles, which supplies four million people with water. Southern California sewage undergoes rigorous cleansing to remove bacteria and nitrogen, and recycled wastewater added to the drinking water supply meets all government standards. But water officials are discovering the medications as they become capable of detecting smaller amounts of chemicals. Because the medications have been found in very small amounts, scientists suspect there is little or no human danger. But they say no one knows if there are health hazards from ingesting small doses of drugs continuously over a lifetime.
Source: http://www.mercurynews.com/mld/mercurynews/news/breaking_new s/13749220.htm

[Return to top]

Public Health Sector

25. *February 01, New York Times* — **Bird flu case in Hong Kong raises questions about China.** A chicken illegally smuggled across the border from mainland China has died of the H5N1 strain of bird flu, Hong Kong officials announced Wednesday, February 1, in a case that raises new questions about whether Chinese provincial officials are concealing the true extent of the disease. A villager living a mile from the Chinese border obtained the chicken Thursday, January 26, from a mainland relative in neighboring Guangdong province, which denies having the disease. The chicken fell sick and died on Tuesday, January 31, said Thomas Sit, Hong Kong's assistant director of agriculture, fisheries and conservation. Hong Kong health officials have alerted their colleagues in Guangdong in an effort to trace the bird's movements. The bird died in a narrow, rural buffer zone along the Guangdong border that is closed to the general public because some of the zone's residents are allowed to move back and forth among farms on both sides of the border. There has been no sign of bird flu in Hong Kong's extensive poultry industry. But three non−migratory birds −− two oriental magpies and a crested mynah −− have been found dead in public places fairly close to the Guangdong border in the past two weeks.
Source: http://www.nytimes.com/2006/02/01/international/asia/01cnd−flu.html?_r=1&oref=slogin

26. *February 01, National Institute of General Medical Sciences* — **New teams join network to model infectious outbreaks.** Four new scientific teams joined the Models of Infectious Disease Agent Study (MIDAS) network, which is developing computer−based simulations of infectious disease outbreaks, the National Institute of General Medical Sciences (NIGMS) announced

Wednesday, February 1. The University of California, Irvine, and the U.S. Centers for Disease Control and Prevention will analyze past transfers of flu from birds to people and model the effects of rapid pathogen evolution on strategies for disease surveillance, prediction, and control. The Harvard School of Public Health, the University of Hong Kong, the National Institute of Public Health and the Environment in the Netherlands, and the University of Washington will use mathematical models to explore mechanisms of transmission, evaluate public health measures, and design methods for monitoring the early stages of an outbreak in real time. The University of Pennsylvania School of Veterinary Medicine and the University of Warwick in the United Kingdom will develop spatial and temporal models of infectious animal diseases. The Harvard Pilgrim Health Care, Harvard School of Public Health, Brigham & Women's Hospital, Kaiser Permanente Northern California, and the National Institute of Infectious Diseases in Argentina will develop ways to identify new clusters of emerging infectious diseases and track antimicrobial resistance in hospitals and ambulatory settings.
Source: http://www.nih.gov/news/pr/feb2006/nigms−01.htm

27. *February 01, Associated Press* — **Polio eradicated in Egypt and Niger.** Polio has been stamped out in Egypt and Niger, leaving just four nations in the world where the disease is endemic, the World Health Organization (WHO) said Wednesday, February 1. The polio virus has not infected anyone in the two African countries during the last 12 months, leaving only Afghanistan, India, Nigeria, and Pakistan as countries where the disease is still classified as endemic −− meaning it has always been present there, the WHO said. Polio is still present in eight other countries −− including Yemen, Indonesia and Somalia −− where it had previously been eradicated before being imported again from one of the endemic countries, WHO said. WHO failed to meet its long−standing target of eradicating polio globally by the end of 2005, in part because Islamic clerics in northern Nigeria led an immunization boycott in 2003. The Nigerian vaccine boycott was blamed for causing an outbreak that spread the disease across Africa, into the Middle East and then into Indonesia. Vaccination programs began again in Nigeria in July 2004. Last year, 1,880 people were infected with polio around the world. When WHO launched the anti−polio campaign in 1988, the worldwide case count was more than 350,000 annually.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://www.usatoday.com/news/world/2006−02−01−polio_x.htm

28. *February 01, Sunday Times (South Africa)* — **Mysterious disease hits North West villages.** A mysterious skin−worm sickness has hit several villages around Mafikeng in North West, South Africa, health officials said. "We have never experienced anything like this," said provincial health spokesperson Tebogo Lekgethwane. "People come to clinics complaining that their body is itching. Within three days small sores develop. A yellow spot then develops from each sore as it gets ripe. Once the sore is expressed a worm comes out of it." The North West health department warned villages around Mafikeng to report to a clinic when noticing small, yellow sores. People from villages near Mafikeng were being treated since December 2005 for the condition. "During visits to the homes of these people, it was found that dogs were also affected," said Lekgethwane. The department of agriculture's veterinary public health and animal unit had taken specimens of the worms to identify their origin.
Source: http://www.sundaytimes.co.za/zones/sundaytimesNEW/newsst/newsst1138767790.aspx

29. *February 01, Agence France−Presse* — **Madagascar fears outbreak of crippling disease.** Madagascan health officials said they fear a outbreak of a crippling mosquito−borne disease that has ravaged the nearby Indian Ocean island of Reunion. Dozens of people showing possible symptoms of the viral infection known as chikungunya have flocked to the main hospital on the island's second city of Toamasina. "The patients have fever but I cannot yet say whether they are suffering from malaria or chikungunya, it is just a suspicion," said Dr. Givance, the hospital chief. Roland Rajonson, the secretary general of Madagascar's health ministry, said that physicians from the capital had been sent to Toamasina on the east coast to look into the matter and would report back by the end of the week. "Tuesday, January 31, we deployed a team of doctors to the ground to investigate whether there were real cases of chikungunya," he said. Chikungunya is Swahili for "that which bends up" and refers to the stooped posture of those afflicted by the crippling disease for which there is no known vaccine or cure. Chikungunya outbreaks have sparked deep concerns in the French territory of Reunion, 500 miles east of Madagascar, where at least 30,000 people are thought to have been taken ill since March.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://news.yahoo.com/s/afp/20060201/hl_afp/madagascarhealth_060201172703;_ylt=AjcFV2YJvnaPH3oi3bwJeAiJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

30. *January 31, U.S. Northern Command* — **U.S. Northern Command prepares for possible pandemic.** U.S. Northern Command recently hosted representatives from more than 40 international, federal, and state agencies for an exercise designed to provoke discussion and determine what governmental actions, including military support, would be necessary in the event of an influenza pandemic in the U.S. "We're building the knowledge base, trying to get ahead of the curve now as much as we can," said Gene Pino, director of USNORTHCOM's training and exercise directorate. Exercise attendees analyzed topics such as public health care, maintaining civil order, and providing continuity of government and private operations in case of widespread infection and worker absenteeism. One of USNORTHCOM's most critical missions during a possible pandemic is to keep the American public informed. The command will work with the Department of Defense, the Department of Health and Human Services, and other agencies at federal, state, and local levels and will use a variety of methods, including traditional press releases and USNORTHCOM's public Website, to disseminate information, said Michael Perini, director of USNORTHCOM public affairs. Exercise participants agreed that the U.S. will not be able to keep a pandemic influenza from entering the country.
Source: http://www.northcom.mil/index.cfm?fuseaction=news.showstory&storyid=21BD7801−99A1−25BB−0DF3CC29B91A0B49

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

31. *February 01, Government Technology* — **Kentucky region to upgrade 911 services.** Kentucky Governor Ernie Fletcher recently presented a $455,058 homeland security check to the city of West Liberty to purchase equipment that will upgrade the region's 911 system. The counties included in the 911 service area include Morgan, Magoffin and Wolfe Counties. "When an emergency occurs, 911 service is the link between first responders and the communities they serve," said Gov. Fletcher. "This grant will work to ensure that this community and the surrounding counties will have the upgraded 911 service that will enable them to be ready and prepared for emergencies." This funding will be used specifically to upgrade the region's E911 capabilities. E911 is an enhanced emergency technology that allows the dispatcher to immediately identify the telephone number and location of a cell phone caller. Such an enhancement is vital in emergencies in which the caller can't talk or is panicking and can't get the necessary information to the dispatcher. The current E911 service in this area is prone to downtime and Magoffin and Wolfe currently have no E911 service. The upgrades to the system in the City of West Liberty will eliminate the downtime problems and will provide coverage to Magoffin and Wolfe Counties.
Source: http://www.govtech.net/news/news.php?id=98202

32. *February 01, WKYT 27 (KY)* — **Earthquake preparedness week in Kentucky.** Kentucky Governor Ernie Fletcher and officials from the Kentucky Office of Homeland Security, Kentucky National Guard, Kentucky Division of Emergency Management and Education Cabinet proclaim February 1− 8, 2006, as Earthquake Preparedness Week. To prepare for this threat, the Kentucky Office of Homeland Security is developing two earthquake exercises in 2006. One exercise will cover Morehead in the east −− the same area as the 1812 quake. The other will be held in the New Madrid Fault Area to the west. Both events will test Kentucky's emergency responders and communities, emergency communications, school evaluation plans and private sector infrastructure restoration, as well as public health, hospital and environmental support. Kentucky Emergency Management has scheduled several events throughout the state during Earthquake Preparedness Week.
Details of Earthquake Preparedness Week:
http://www.kyem.ky.gov/programs/Earthquake/default.htm
Source: http://www.wkyt.com/Global/story.asp?S=4438413&nav=4CAL

33. *February 01, Government Accountability Office* — **GAO−06−365R: Preliminary Observations on Hurricane Response (Correspondence).** In recent months, the Government Accountability Office (GAO) has undertaken a body of work to address federal, state, and local preparations for, response to, and recovery from Hurricanes Katrina and Rita. The purpose of this document is to provide some preliminary observations based on GAO's work to date. There are several key themes that, based on GAO's current preliminary work, underpin many of the challenges encountered in the response to Hurricane Katrina and reflect certain lessons learned from past disasters. The following three key themes seem to be emerging. First, prior to a catastrophic event, the leadership roles, responsibilities, and lines of authority for the response at all levels must be clearly defined and effectively communicated. Second, to best position the nation to prepare for, respond to, and recover from major catastrophes, there must be strong advanced planning, both within and among responder organizations, as well as robust training and exercise programs to test these plans in advance of a real disaster. Third, response and recovery capabilities needed during a major catastrophic event differ significantly from those required to respond to and recover from a “normal disaster.” These capabilities require better

contingency plans and the resources to carry them out.
Source: http://www.gao.gov/new.items/d06365r.pdf

34. *January 31, Lompoc Record (CA)* — **Mock hostage scenario practiced in California.** In a Santa Barbara County Sheriff's Department training exercise, a downtown Solvang bank was “robbed” Monday, January 30. The departmentwide exercise, with nearly 100 participants, “put skills to the test,” Sheriff Jim Anderson said. Participants included patrol units, the SWAT team, the criminal investigation division, hostage negotiators, a communications unit and helicopter unit, as well as Valley substation commanders. After a briefing by Special Operations Division Commander Don Patterson, the scenario began. Members of the Santa Barbara city SWAT team portrayed the hostages and suspects. Patterson said preparation for the exercise began four months ago. A command post was established and intelligence, including aerial photos of the area and other information, was processed to develop a plan. At the conclusion of the exercise, four suspects were taken into custody, the fifth suspect, with a bombed strapped to his body, approached deputies and was killed. All 10 hostages were released. Sgt. Tom Walton, Emergency and Planning Preparedness, said evaluators will come together in the upcoming weeks for a full debriefing to analyze all segments of the situation response.
Source: http://www.lompocrecord.com/articles/2006/01/31/news/news07. txt

35. *January 31, Miami Herald (FL)* — **Miami police hold anthrax attack drill.** A simulated anthrax attack rocked Miami police headquarters Tuesday morning, January 31 −− part of a series of ongoing spot drills designed to test and train the department for a potential weapons of mass destruction (WMD) attack, police said. The surprise drill −− dubbed "Operation Pigeon Drop" −− emptied nearly all of the five−story headquarters building for almost two hours. The exercise aimed to ensure that all police employees are able to recognize, respond to and recover from an internal WMD incident, the department said in a release. Practice alarms first sounded around 8 a.m. EST, when an unsuspecting employee on a routine mail run opened a letter −− only to find white powder inside, police said. Terror alert plans then kicked into gear, setting in motion procedures to secure the crime scene and evacuate the building. Miami Fire Rescue runs similar exercises several times a year, but Tuesday marked the most sweeping simulation of an internal WMD attack that Miami police have ever had, police spokesperson Herminia Salas−Jacobson said. Police emergency management teams are now reviewing the department's performance, preparing an after−action analysis of its strong and weak points, police said.
Source: http://www.miami.com/mld/miamiherald/13756014.htm

36. *January 31, Associated Press* — **Indiana faces questions in homeland security audit.** Indiana already has addressed many of the concerns outlined in a federal audit of how the state used anti−terrorism grants in 2002 and 2003, the state's homeland security director said. A summary of the audit, conducted between November 2004 and April 2005, was released Monday, January 30. The report said Indiana "attempted to conscientiously manage" first−responder grant programs but did not follow its approved strategic plan and did not aggressively manage the programs. It also said most of the counter−terrorist response kits, bought by the State Emergency Management Agency for $4.5 million in December 2002, still had not been distributed to first responders as of January 2005. The federal agency awarded Indiana about $48 million for the 2002 and 2003 fiscal years. Spending included almost $1 million in equipment that might not have been approved for purchase, or possibly not used as intended,

and $278,857 in undocumented overtime for police agencies. Fifteen Indiana communities had at least $10,000 still in question as of last September, several months after the state sent letters to many communities asking them to explain how their money had been spent and to return what remained.
Source: http://www.wabashplaindealer.com/articles/2006/01/31/state_n ews/state3.txt

[Return to top]

Information Technology and Telecommunications Sector

37. *February 01, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−032A: Winamp Playlist Buffer Overflow.** Systems affected: Microsoft Windows systems with Winamp 5.12 or earlier. Overview: America Online has released Winamp 5.13 to correct a buffer overflow vulnerability. Exploitation of this vulnerability could allow a remote attacker to execute arbitrary code with the privileges of the user. Impact: By convincing a user to open a specially crafted playlist file, a remote unauthenticated attacker may be able to execute arbitrary code with the privileges of the user. Winamp may open a playlist file without any user interaction as the result of viewing a Webpage or other HTML document.
Solution: Upgrade to Winamp 5.13: http://www.winamp.com/player/
Source: http://www.uscert.gov/cas/techalerts/TA06−032A.html

38. *January 31, Security Tracker* — **HP Tru64 UNIX BIND flaw may let remote users gain privileged access.** A vulnerability was reported in BIND on HP Tru64 UNIX. A remote user may be able to gain access on the target system. An unspecified vulnerability exists in the HP Tru64 UNIX operating system when running DNS BIND and configured as a DNS BIND name server. A remote user can gain privileged access. Solution: HP has issued Early Release Patch kits (ERPs). See source Website for more details.
Source: http://www.securitytracker.com/alerts/2006/Jan/1015551.html

39. *January 31, Security Focus* — **Perl Perl_sv_vcatpvfn format string integer wrap vulnerability.** Perl is susceptible to a format−string vulnerability. This issue is due to the programming language's failure to properly handle format specifiers in formatted printing functions. An attacker may leverage this issue to write to arbitrary process memory, facilitating code execution in the context of the Perl interpreter process. This can result in unauthorized remote access. Developers should treat the formatted printing functions in Perl as equivalently vulnerable to exploitation as the C library versions, and should properly sanitize all data passed in the format specifier argument. Solution: Webmin has released updated versions of Webmin and Usermin to fix the insecure usage of the formatted printing functions.
See the following Website for more solution details:
http://www.securityfocus.com/bid/15629/solution
Source: http://www.securityfocus.com/bid/15629/discuss

40. *January 31, Reuters* — **Israel holds couple in corporate espionage case.** An Israeli couple suspected of masterminding a computer virus that set off a major industrial espionage investigation was repatriated for trial on Tuesday, January 31, under an extradition deal with

Britain, police said. Michael and Ruth Haephrati were arrested in their London home last year over allegations that a Trojan horse program they had developed was bought by private investigators who helped top Israeli corporations spy on each other's computers. Israeli police spokesperson Mickey Rosenfeld said the couple flew in overnight after Britain approved their extradition. Tel Aviv Magistrate's Court ordered them placed in custody for 10 days so that they could be interrogated by police. Computer hacking carries a maximum five year jail term in Israel, which can be increased if data theft is involved. At least 18 other Israelis have been questioned in the Trojan horse case, including corporate executives. Several private investigators have been indicted on related charges. Among companies probed by police in connection with the case were Israel's top mobile phone operator, Cellcom, and two subsidiaries of phone company Bezeq Israel Telecom −− cellular operator Pelephone and the satellite television provider YES. All of the firms denied any wrongdoing.
Source: http://today.reuters.com/news/NewsArticle.aspx?type=technologyNews&storyID=2006−01−31T121453Z_01_L31454049_RTRUKOC_0_US−CRIME−ISRAEL−SPYWARE.xml

41. *January 31, Tech World* — **Browsers face triple threat.** Polish security researcher Michael Zalewski has highlighted three bugs in the handling of cookies that he says could be used to carry out attacks on commercial Websites. The bugs, for which Zalewski has coined the term "cross site cooking," are fundamental to the design and implementation of cookies. The first problem involves the way browsers handle the domain specified in a cookie. Browsers should theoretically reject cookies where the domain is specified too broadly, but the mechanism doesn't work in Mozilla−based browsers, though Internet Explorer doesn't seem to be affected, Zalewski said. A variant on this bug is that browsers don't check to see if anything is between the periods in a domain name specified by a cookie. The third problem Zalewski outlined is a trick that he said could be easily used to force random visitors to a site to accept and relay malicious cookies to third−party sites. "Using this trick, a brand new identity may be temporarily bestowed upon the user, and used to perform certain undesirable or malicious tasks on the target site," he said.
Source: http://www.techworld.com/security/news/index.cfm?NewsID=5276&Page=1&pagePos=6&inkc=0

42. *January 31, eWeek* — **Oracle completes Siebel merger.** It's official: Oracle confirmed that it completed the acquisition of Siebel Systems late in the day Tuesday, January 31, after 99 percent of shareholders voted to accept the $5.85 billion deal. "Oracle's focus on modern, standards−based applications and middleware is moving us into a leadership position in applications and on−demand services. Siebel accelerates that move," Oracle CEO Larry Ellison said in a statement. Oracle announced its intent to acquire Siebel in September of last year. While the company has been scarce on details, primarily out of necessity, it has said it will utilize Siebel's CRM technology as the basis for its next generation Fusion CRM suite of applications. Oracle will also maintain Siebel's separate on−demand CRM code, though it's not clear how either code line will be integrated with Oracle's existing −− and overlapping −− on−premises and on−demand software.
Source: http://www.eweek.com/article2/0,1895,1917371,00.asp

43. *January 30, Small Business Pipeline* — **Small businesses get four times the spam of larger enterprises.** Small companies were sent almost 50 spam e−mails per day per user in 2005, up

from 36 in 2004. This represents four times the number that employees at large companies were sent daily on average last year (12 per user per day in 2005 versus three in 2004). This is according to an annual report by Postini, a provider of message management solutions. The reason for this is that smaller businesses are more prevalent in targeted industries such as publishing, advertising, legal, and real estate, according to Andrew Lochart, senior director of marketing at Postini. "These are industries where you have 100 percent white collar workers whose e−mail addresses are very well known in the world," said Lochart. Another theory is that spammers may presume that larger companies are able to afford strong anti−spam measures, and may not try to infiltrate them as frequently, said Lochart. "What makes it a problem, regardless of why, is that smaller companies are the ones who have fewer defenses in place," said Lochart. "There are no large dedicated IT staffs in place, or large budgets for technology, so it's a double whammy."
Postini original press release: http://www.postini.com/news_events/pr/pr013006_tr.php
Postini's Annual Message Management and Threat Report:
http://www.postini.com/whitepapers/?WPID=36
Source: http://www.smallbizpipeline.com/showArticle.jhtml?articleID= 177105260

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT continues to contact and receive reports from federal agencies that have been affected by the CME−24 virus. The CME−24 worm actively disables anti−virus software on a host system and will also overwrite users' data files on the third of every month. This virus affects all recent versions of Microsoft Windows.

The CME−24 worm spreads primarily by harvesting email addresses from files on the local machine and then emailing itself as an executable attachment. It uses subject lines such as "Photos", "*Hot Movie*", and "Miss Lebanon 2006" to entice the user into opening the attachment. As soon as the attachment is executed, the user's system is immediately infected. Infected hosts within a network enclave will also try to spread locally through network shares with weak passwords.

On the third of every month, CME 24 will over write users' files on all accessible drives with the message "DATA Error [47 0f 94 93 F4 F5]". This will happen approximately 30 minutes after the user logins to the infected machine. The files affected by this variant will have the following file extensions: .doc, .xls, .mdb, .md3, .ppt, .pps, .zip, .rar, .pdf, .psd, and .dmp.

Agencies that observe communication from internal machines to the 207.172.16.155 address should investigate further to determine if these machines are infected. Several agencies have reported that the systems that were impacted had anti−virus

but were not running the latest signatures.

US−CERT recommends the following course of action:

Ensure that the latest anti−virus definitions are loaded on servers and workstations.

Leverage Internet Content Filtering Solutions to block executable and unknown file types at the email gateway

Setting up an access control list to detect users from browsing to the aforementioned websites/IP addresses. LURHQ provides snort signatures related to the CME−24 worm on their Website.

Monitoring of outbound traffic to identify potential malicious traffic or information leaks.

The infected host will also access a website with a web counter. This web counter shows how many machines have been infected, although it is expected that an infected machine may access the website on multiple occasions, thus inflating the number. The original web counter showed consistent growth with over 500,000 infections on Saturday and is now currently showing over 700,000 infections. However, recent web log postings suggest that the number is much closer to 300,000 unique addresses. FBI agents have received log data that resided on the web server, and is sharing the bulk data with US−CERT for analysis.

Please report any validated agency connection to the 207.172.16.155 website during the last 30 days to the US−CERT for further correlation and analysis.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 27015 (halflife), 139 (netbios−ssn), 135 (epmap), 25 (smtp), 6346 (gnutella−svc), 54000 (−−−), 4142 (oidocsvc) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

44. *February 01, Chicago Sun Times (IL)* — **Mayor: Cameras will make us safer.** Chicago Mayor Richard Daley on Monday, January 31, embraced a radical plan to require every licensed Chicago business open more than 12 hours a day to install indoor and outdoor cameras. "Block clubs, community organizations want cameras. ... They can't walk down the street. ... You can't walk to church. You can't get on the CTA. ... Cameras really prevent much crime. Cameras also solve a lot of crime," Daley said. Chicagoland Chamber of Commerce

President Jerry Roper estimated that 12,000 businesses −− maybe more −− are open for more than 12 hours a day and, therefore, would be covered by the sweeping camera mandate. That includes roughly 7,000 restaurants, more than 100 hotels and scores of retail establishments. If the mayor's endorsement translates into City Council approval of the ordinance, business leaders will demand tax breaks and a phase−in similar to the sprinkler ordinance that gives older high−rises 12 years to comply, Roper said.
Source: http://www.suntimes.com/output/news/cst−nws−camera31.html

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.